

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

2019 MAY -8 AM 9:50

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)IN THE MATTER OF THE SEARCH OF INFORMATION
ASSOCIATED WITH RSand5401@gmail.com, AND THAT
IS STORED AT PREMISES CONTROLLED BY GOOGLE,
INC.

Case No.

2:19mj372

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1001	Making false statements
18 U.S.C. § 1343	Wire fraud
18 U.S.C. § 287	Making false or fraudulent claim against the U.S.
18 U.S.C. § 38	Fraud Involving aircraft parts

The application is based on these facts:

See Affidavit

☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Delia McMullen, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date:

5-8-19

City and state:

Columbus, OH

Judge's signature

Chelsey M. Vascara, Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
RSand5401@gmail.com, AND THAT IS
STORED AT PREMISES CONTROLLED
BY Google, Inc.

Case No. **2:19mj372**

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Delia McMullen, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information, associated with the email account of RSand5401@gmail.com, that are stored at premises controlled by Google, Inc., an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google, Inc. to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Defense Criminal Investigative Service (DCIS), which is part of the Office of the Inspector General for the U.S. Department of Defense (DoD). I have been so employed for approximately 16 years. In my current capacity, I am charged with investigating acts of suspected DoD contract fraud.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code Section 1001 (making false statements); Section 1343 (wire fraud); Section 287 (making a false or fraudulent claim against the U.S); and Section 38 (fraud involving aircraft parts), have been committed by **David Reed, Reed Sales LLC**, and other unknown persons and companies. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

Contracting Process

6. The United States Department of Defense (DoD), contracts through its various agencies, such as the Defense Logistics Agency (DLA). DLA is the United States’ combat logistics support agency, and as such manages the global supply chain for all military services, 10 combatant commands, other federal agencies, and partner and allied nations. DLA has three primary depots that manage the military’s global supply chain – DLA Land and Maritime (L&M) in Columbus, Ohio, DLA Aviation in Richmond, Virginia, and DLA Troop Support (TS) in Philadelphia, Pennsylvania.

7. When the DoD determines that a particular part is needed, the DoD issues “Solicitations,” or Requests for Quotation (RFQs) electronically through a web-based application, DIBBS (DLA’s Internet Bid Board System). Users (potential contractors) are able to search for, view, and submit secure quotes based upon the RFQs for the items DLA is looking to obtain. The solicitations (RFQ’s) list the DoD requirements, which can include drawings and/or specifications such that any potential contractor is aware of exactly how the part is to be made or where they can obtain the part. DoD contractors are required to have a quality control system in place to insure the parts supplied to the DoD are in accordance with DoD drawings and specifications. In addition to noting the contractor’s agreement or disagreement with the requirements of the solicitation, the quote, or bid, submitted will list the contractor name, business location and an email address.

8. In order to conduct business with the DoD, contractors must register in the System for Award Management (SAM), to include providing an email address, and agree to receive payments electronically. The contractors must also obtain a Commercial and Government Entity (CAGE) code. The CAGE code is a 5-character identification number used extensively within the federal government, assigned by the DLA. The CAGE code is used to support a variety of mechanized systems throughout the government and provides a standardized method of identifying a given contractor facility at a specific location.

9. In the contracting process, once parts are shipped to the DLA, contractors enter the shipping and invoicing information electronically, through a secure, web-based system, which allows the government to receive and pay electronically. Upon receiving the invoice, the DoD, through the Defense Finance and Accounting Service (DFAS), Columbus, Ohio; in the

Southern District of Ohio, will issue electronic payment to the supplying contractor and retain a voucher as a record of the payment.

10. DLA L&M in Columbus is also home to laboratories used to test and identify nonconforming parts sold to DLA, including the capability to test for counterfeit material, substitute inferior products, and remark/over brand items. These laboratories at DLA L&M are used to test all suspect parts provided to DLA worldwide.

Reed Sales LLC

11. **Reed Sales LLC** was formed in Tennessee on August 8, 2013, and the principle address provided to the State for the company was 491 County Road 255, Niota, TN 37826. On August 19, 2013, **Reed Sales** was initially registered in the SAM. The physical and mailing address entered for the company into SAM was 491 County Road 255, Niota, TN 37826 and the President of the company is identified as **David Reed**. During August 8, 2013 through April 23, 2018, approximately 12 modifications of **Reed Sales'** information in the SAM were made, including annual re-registrations of the company in the SAM. In both **Reed Sales'** initial registration in the SAM and all subsequent modifications, **David Reed** was identified as the President of **Reed Sales**, and **Reed Sales'** business office was listed as 491 County Road 255, Niota, TN 37826. Also, in all instances, the individual who entered the information in the SAM – called the “Individual Executing Consent” in the SAM – was **David Reed**.

12. Since September 2013, **Reed Sales** has received \$1.87 million in DLA L&M and DLA Aviation contracts.

13. In November 2018, **David Reed** and **Reed Sales** came to the attention of DLA L&M because the company used an IP address to access DIBBS that matched an IP address used by another DLA contractor whose Point of Contact had been debarred. After learning this,

various parts sold by **Reed Sales** to DLA L&M under five different contracts were pulled from stock and tested. All of the parts – valued at \$36,356 – failed the tests. These parts consisted of electrical connector plugs and circuit breakers used on U.S. military weapon systems, including the F/A-18 aircraft and LGM-30 Minuteman III Missile. The majority of these parts were critical application items, which are items on a U.S. military weapon system that are essential to the weapon's performance, operation, and/or the preservation of life or safety of operating personnel. DCIS subsequently opened a criminal investigation into **Reed Sales** and **David Reed**.

14. DLA L&M identified additional parts received from **Reed Sales**, on three separate contracts valued at \$22,084, which were in DLA L&M stock. DLA L&M pulled and tested these parts as well; all parts failed the tests. These parts consisted of electrical test connectors, circuit breakers, and electrical receptacle connectors used on U.S. military weapon systems, including the Apache Longbow helicopter, AN/TPQ-36 Firefinder Radar Set, and Aircraft Launch and Recovery Equipment (ALRE) systems. All of these parts were critical application items.

15. The above eight contracts, which were issued by DLA L&M to **Reed Sales** during August 31, 2016 through September 13, 2017, and on which **Reed Sales** sold parts to DLA L&M that ultimately failed the tests and could not be used on the intended U.S. military weapon systems, were “code and part” contracts. Contracts issued by DLA are typically one of two types of contracts: “drawing” contracts or code and part contracts. On a drawing contract, the contractor is required to manufacture a specific part in accordance with specifications identified by DLA in its solicitation and contract. On a code and part contract, the contractor is required to provide DLA a specific part that was manufactured by an approved source; DLA identifies the

specific part and approved source(s) in its solicitation and contract. All of the above eight DLA contracts with DLA were code and part contracts. **Reed Sales** was required to provide DLA specific parts manufactured by approved sources, but instead sold inferior parts from unapproved sources.

16. For example, one of the DLA L&M contracts was for 126 electrical test connectors, critical application items used on the AH-64-D Apache Longbow helicopter. DLA L&M was able to test 10 of these connectors, which revealed the parts provided by **Reed Sales** were the completely wrong part. **Reed Sales** was required to provide the correct connector from the approved source, TYCO Connectivity Corporation. Instead, **Reed Sales** provided a commercial, off-the-shelf Snap-Tite Saddlegrip connector manufactured by Arlington Industries. Per the test report, "The Substitute item supplied is available at Home Depot for \$2.35 but the contract price we paid was \$45.66."

17. In its bids for the above 8 contracts, **Reed Sales** certified to DLA that it would provide the correct part from an approved source. Each quote contains the following "Quoter" information:

Name: **David Reed**
Phone: (423) 744-3030
Email: RSand5401@gmail.com

18. In early April 2019, a DCIS agent contacted DLA Aviation, and learned that **Reed Sales** provided defective parts to DLA Aviation on 14 known contracts, cumulatively valued at \$262,497. The majority of these parts were critical application items, and the majority of contracts were code and part contracts. DLA Aviation is pulling additional parts sold by **Reed Sales** from stock and suspects these parts are defective as well.

19. The majority of these 14 DLA Aviation contracts were code and part contracts; in its bid for each code and part contract, **Reed Sales** certified to DLA that it would provide the correct part from an approved source. Further, each quote in all 14 DLA Aviation contracts contains the following “Quoter” information:

Name: **David Reed**
Phone: (423) 744-3030
Email: RSand5401@gmail.com

20. On March 28, 2019, DLA Headquarters debarred **Reed Sales** and **David Reed** from contracting with the executive branch of the Federal Government for a period of three years.

21. A query in the CLEAR database on the above phone number revealed that this phone number comes back to **David Reed** at 491 County Road 255, Niota, TN 37826. The CLEAR report cites three sources which reported this same information – Household Living, Dun and Bradstreet, and Worldbase Detail.

22. **David Reed’s** driver’s license information also disclosed a residence for **Reed** at 491 County Road 255, Niota, TN 37826.

23. On February 4, 2019, a DCIS agent served a preservation letter on Google, Inc., which acknowledged receipt, to preserve the email account of RSand5401@gmail.com. In general, an email that is sent to a Google, Inc. subscriber is stored in the subscriber’s “mail box” on Google, Inc. servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google, Inc. servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google, Inc.’s servers for a certain period of time.

BACKGROUND CONCERNING EMAIL

24. In my training and experience, I have learned that Google, Inc. provides a variety of on-line services, including electronic mail ("email") access, to the public. Google, Inc. allows subscribers to obtain email accounts at the domain name gmail.com, like the email account[s] listed in Attachment A. Subscribers obtain an account by registering Google, Inc. During the registration process, Google, Inc. asks subscribers to provide basic personal information. Therefore, the computers of Google, Inc. are likely to contain stored electronic communications (including retrieved and unretrieved email for Google, Inc. subscribers) and information concerning subscribers and their use of Google, Inc. services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

25. A Google, Inc. subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google, Inc. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

26. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information

can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

27. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

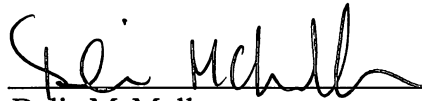
28. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

29. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

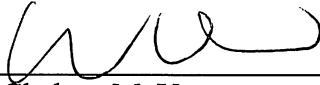
30. I submit that this affidavit supports probable cause for a warrant to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B. Because the warrant will be served on Google, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Delia McMullen
Special Agent
Defense Criminal Investigative Service

Subscribed and sworn to before me on May 8, 2019



Honorable Chelsey M. Vascara
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with email account RSand5401@gmail.com, that are stored at premises owned, maintained, controlled, or operated by Google, Inc., a company headquartered at Google, Inc., Attn: Custodian of Records, 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on February 4, 2019, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the accounts from August 8, 2013 through the present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Section 1001 (making false statements), Section 1343 (wire fraud), Section 287 (making a false or fraudulent claim against the U.S), and Section 38 (fraud involving aircraft parts), those violations involving **David Reed, Reed Sales LLC**, and other known and unknown persons and companies, and occurring after August 8, 2013, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- Information related to U.S. Department of Defense (DoD) contracting, to include but not limited to, solicitations, bids/quotes, purchase orders/contracts, DFAS or other payment records, inspection records or results including any drawings or certifications whether conducted in-house or by a government agency such as DCMA or a private third-party; traceability documents or requests for traceability; the ordering or manufacturing of any parts provided to the DoD including any receipts, invoices, correspondence with suppliers; the shipping of parts from suppliers and to the DoD.
- Information related to the creation, ownership, registration, corporate meeting minutes, tax records and annual reports, employees or dissolution of **Reed Sales LLC**; the extent of their dealings with the DoD and any of its agencies to include any records of CAGE code or SAM applications or registrations, pre-award survey documents, quality manuals and correspondence with DoD;
- Records and information relating to fraud committed against the DoD and any of its agencies;

- Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, Inc., and my title is _____ . I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google, Inc. The attached records consist of _____ . I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, Inc., and they were made by Google, Inc. as a regular practice; and

b. such records were generated by Google, Inc.'s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google, Inc. in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, Inc., and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature